Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	This morning, the multimedia company experienced a **DoS (Denial of Service) attack** that overwhelmed the internal network for approximately two hours. The attack was caused by a flood of incoming **ICMP packets** targeting an unconfigured firewall. This resulted in network services becoming unresponsive, preventing normal internal traffic from accessing critical resources. The incident management team resolved the event by blocking incoming ICMP packets and taking non-critical services offline while restoring critical network operations.
Identify	The incident management team identified the attack as an **ICMP flood (DoS)**. The primary vulnerability was an **unconfigured firewall**, which allowed a malicious actor to overwhelm the system with ping requests. The affected systems included the **internal network infrastructure**, causing a total service outage for two hours.
Protect	**To prevent a recurrence, the team has implemented several safeguards:** **• Firewall Maintenance: Configured new rules to limit the rate of incoming ICMP packets.** **• Source IP Verification: Implemented verification on the firewall to check**

	for and block spoofed IP addresses. **• IDS/IPS System: Deployed an Intrusion Detection/Prevention System to filter suspicious ICMP traffic based on defined characteristics.**
Detect	The organization has enhanced its monitoring capabilities to detect similar anomalies faster: • **Network Monitoring Software**: Installed specialized software to detect abnormal traffic patterns in real-time. • **Security Continuous Monitoring**: The IDS/IPS system will continuously scan for suspicious ICMP characteristics and alert IT staff of security events.
Respond	In the event of a future attack, the following response plan will be executed : • **Mitigation**: Affected resources or non-critical services will be taken offline or isolated immediately to preserve critical systems. • **Neutralization**: Firewall rules will be dynamically adjusted to block verified malicious source IPs. • **Analysis**: Security logs and monitoring data will be analyzed to identify the attack's origin and path.
Recover	Recovery procedures focus on returning to normal operations swiftly : • **Restoration**: The network security team will prioritize the restoration of critical network services first, followed by non-critical assets. • **Improvement**: Post-incident audits will be conducted to identify if additional

	firewall rules or IPS signatures are needed based on the latest threat data.

Reflections/Notes: Applying the **NIST CSF** core functions (Identify, Protect, Detect, Respond, and Recover) ensures a proactive and structured approach to managing cybersecurity risks. By moving from a reactive "unconfigured" state to a proactive monitoring and filtering posture, the organization significantly reduces the impact and duration of potential future DoS attacks.